

A

$$\begin{aligned} & \boxed{x \in_R \mathbb{Z}_q} \sim 102 \\ & \boxed{X = g^x \bmod p} \sim 104 \end{aligned}$$

$$\xrightarrow{\quad \quad \quad X \quad \quad \quad}$$

$$\boxed{S = Y^x \bmod p} \sim 114$$

B

$$\begin{aligned} & \boxed{y \in_R \mathbb{Z}_q} \sim 108 \\ & \boxed{Y = g^y \bmod p} \sim 110 \\ & \boxed{S = X^y \bmod p} \sim 116 \end{aligned}$$

$$\xrightarrow{\quad \quad \quad Y \quad \quad \quad}$$

FIG. 1

A

$$\begin{aligned} x &\in_R \mathbb{Z}_q \sim 202 \\ m &= g^x \cdot (H_1(A, B, \pi))^r \bmod p \sim 204 \end{aligned}$$

$\underbrace{\hspace{1.5cm}}_m \xrightarrow{\hspace{1.5cm}}$

$$\begin{aligned} \sigma &= \mu^x \bmod p \sim 220 \\ \text{TEST} - k' &\stackrel{?}{=} H_{2a}(A, B, m, \mu, \sigma, \pi) \sim 222 \\ k' &= H_{2b}(A, B, m, \mu, \sigma, \pi) \sim 224 \\ K &= H_3(A, B, m, \mu, \sigma, \pi) \sim 226 \end{aligned}$$

$\underbrace{\hspace{1.5cm}}_{k'} \xrightarrow{\hspace{1.5cm}}$

$\underbrace{\hspace{1.5cm}}_{\mu, k} \xrightarrow{\hspace{1.5cm}}$

B

$$\begin{aligned} \text{TEST} - m &\stackrel{?}{=} 0 \bmod p \sim 208 \\ y &\in_R \mathbb{Z}_q \sim 210 \\ \mu &= g^y \bmod p \sim 212 \\ \sigma &= \left( \frac{m}{(H_1(A, B, \pi))^r} \right)^y \bmod p \sim 214 \\ K &= H_{2a}(A, B, m, \mu, \sigma, \pi) \sim 216 \end{aligned}$$

$$\begin{aligned} \text{TEST} - k' &\stackrel{?}{=} H_{2b}(A, B, m, \mu, \sigma, \pi) \sim 230 \\ K &= H_3(A, B, m, \mu, \sigma, \pi) \sim 232 \end{aligned}$$

FIG. 2

A

$$x \in \mathbb{Z}_q \sim 302$$

$$h \in \mathbb{Z}_p^* \sim 304$$

$$m = g^x \cdot h^y \cdot H_1(A, B, \pi) \sim 306$$

$$\sim 308 \quad m$$

B

$$\text{TEST } m \neq 0 \bmod p \sim 310$$

$$y \in \mathbb{Z}_q \sim 312$$

$$\mu = g^y \bmod p \sim 314$$

$$\sigma = \left( \left( \frac{m}{H_1(A, B, \pi)} \right)^y \right)^{y^{-1} \bmod q} \sim 316$$

$$K = H_{2a}(A, B, m, \mu, \sigma, \pi) \sim 318$$

$$\mu, K \quad 320$$

$$\sigma = \mu^x \bmod p \sim 322$$

$$\text{TEST } K \stackrel{?}{=} H_{2a}(A, B, m, \mu, \sigma, \pi) \sim 324$$

$$K' = H_{2b}(A, B, m, \mu, \sigma, \pi) \sim 326$$

$$K = H_3(A, B, m, \mu, \sigma, \pi) \sim 328$$

$$K' \quad 330$$

$$\text{TEST } K' \stackrel{?}{=} H_{2b}(A, B, m, \mu, \sigma, \pi) \sim 332$$

$$K = H_3(A, B, m, \mu, \sigma, \pi) \sim 334$$

FIG. 3

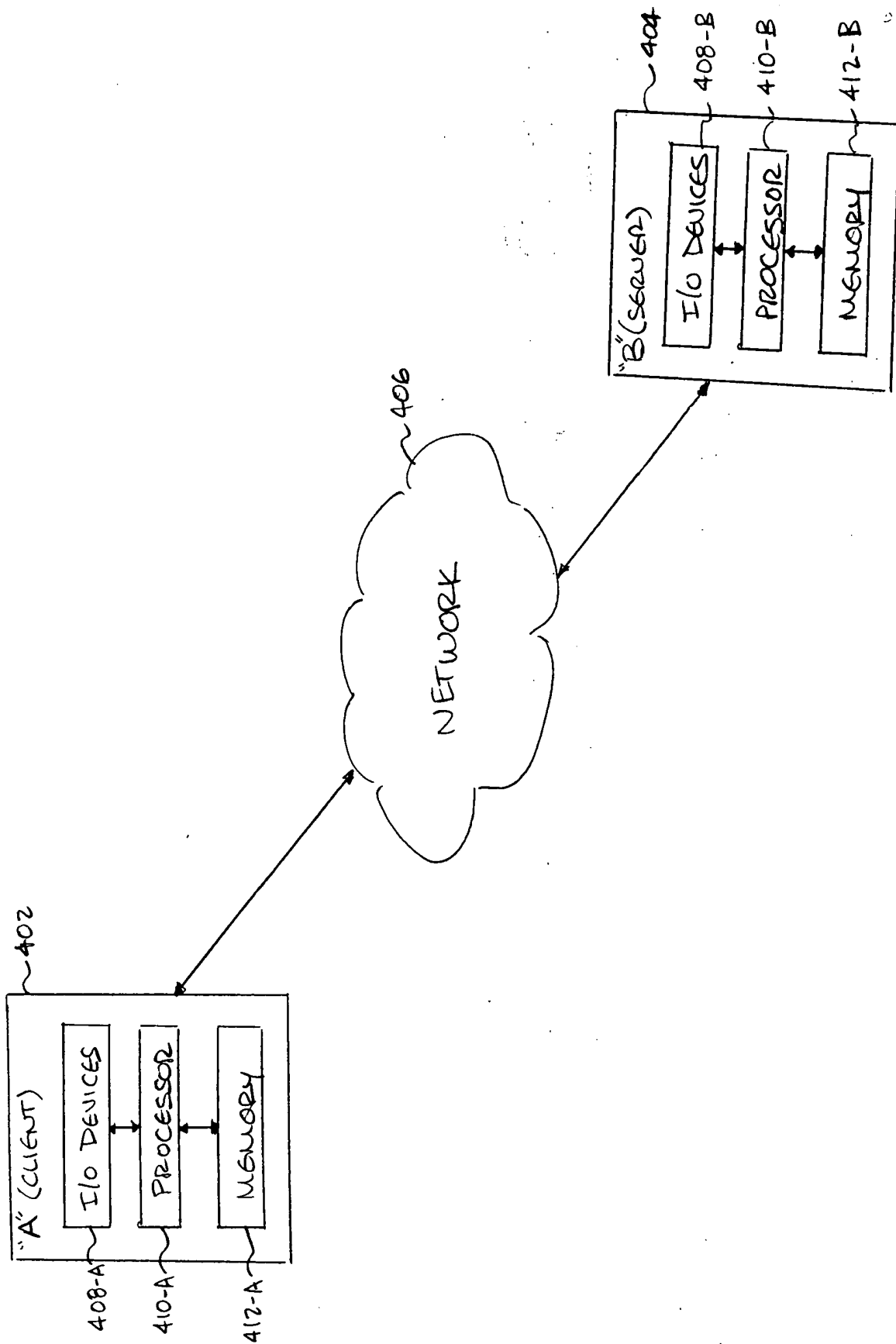


FIG. 4